A BOUND FOR THE NILPOTENCY CLASS OF A FINITE p-GROUP IN TERMS OF ITS COEXPONENT

PAUL J. SANDERS AND TOM S. WILDE

1. Introduction

For a prime p and a finite p-group P, we define the **coexponent** of P to be the least integer $f(P)$ such that P possesses a cyclic subgroup of index $p^{f(P)}$, and the purpose of this paper is to derive a bound for the nilpotency class in terms of the coexponent. Observe that such a bound is possible only for odd primes since if $n > 2$, the group $C_{2^{n-1}} \rtimes C_2$ with the cyclic group of order 2 acting by inversion, is a group of order 2^n which has coexponent 1 and (maximal) nilpotency class $n-1$. We prove two theorems in this paper.

Theorem 1. *Let p be an odd prime and P a finite p-group of coexponent $f(P) \geq 1$. Then $cl(P) \leq 2f(P)$.*

From this it follows that if P is a finite p-group with $p > 2f(P)$ then the group can be regarded as a Lie ring by "inverting" the Baker–Campbell–Hausdorff formula (see [4] and [3]). This transformation to a Lie ring setting is used in [5] to classify the finite p-groups of coexponent 3 for primes greater than 3.

The bound in Theorem 1 is clearly attained by taking P to be a non-Abelian p-group containing a cyclic maximal subgroup (for $p > 2$), and an examination of the proof of Theorem 1 will show that this bound is attained only if $f(P) = 1$ or $p = 3$. We then have

Theorem 2. *Let p be a prime greater than 3 and P a finite p-group of coexponent $f(P) \geq 2$. Then $cl(P) \leq 2f(P) - 1$.*

1991 *Mathematics Subject Classification.* Primary 20D15.

The question of whether a 3-group P exists with coexponent greater than 1 and nilpotency class exactly $2f(P)$ is left open.

2. Proofs

Let p be an odd prime and P a finite p-group of order p^n and coexponent $f = f(P) \geq 1$. It may be assumed that $n > 2f$ since both Theorems are trivially true otherwise. We begin by examining the core of a largest cyclic subgroup contained in P, so let $a \in P$ have order p^{n-f} and define subgroups Q and N of P to be $\langle a \rangle$ and $\mathrm{Core}_P\big(\langle a \rangle\big)$ respectively.

Lemma 1. *Defining integers r and s by $p^r = \min\,\{|P : QQ^b| : b \in P\}$, and $p^{r-s} = |P : C_P(N)|$ we have*

i. $1 \leq r \leq f$ *and* $|P : N| = p^{2f-r}$.
ii. $s \geq 0$, *and* $[[\dots, [N, \underbrace{P], \dots], P]}_{u \text{ times}} \leq \mho_{(n-2f)u}(N)$, *for any integer* $u \geq 1$.

Proof.

i. It is easy to see that no group is the product of two proper conjugate cyclic subgroups and so it follows that $1 \leq r \leq f$. To see that $|P : N| = p^{2f-r}$ observe that for any element b of P we have
$$|Q : Q \cap Q^b| = |QQ^b : Q|.$$
Now since Q is cyclic there exists some element c of P with $\mathrm{Core}_P(Q) = Q \cap Q^c$ and then for any other $b \in P$ we have
$$Q \geq Q \cap Q^b \geq Q \cap Q^c,$$
whence $|QQ^c : Q| \geq |QQ^b : Q|$. Therefore $|Q : N| = \max\,\{|QQ^b : Q| : b \in P\} = p^{f-r}$ and so $|P : N| = p^{2f-r}$.
ii. Let c be defined as in i. Then since N is centralised by both Q and Q^c it follows that $QQ^c \leq C_P(N)$ and so $s \geq 0$. Now let k be an integer satisfying $1 \leq k \leq n - 2f + r$ (observe by i. that $|N| = p^{n-2f+r}$ and $n - 2f + r \geq 2$). Because N is a cyclic group

of prime-power order, any automorphism of $N/\mho_k(N)$ lifts to an automorphism of N and so we have a composite of maps

$$P \xrightarrow{\phi} \mathrm{Aut}(N) \xrightarrow{\gamma} \mathrm{Aut}\left({}^{N}/_{\mho_k(N)}\right)$$

where P acts by conjugation on N and γ is onto. It follows that

$$|\mathrm{Im}(\phi)| = |P : C_P(N)| \quad \text{and} \quad |\mathrm{Ker}(\gamma)| = \frac{p^{n-2f+r-1}(p-1)}{p^{k-1}(p-1)}.$$

Since p is odd we have that $\mathrm{Aut}(N)$ is cyclic, and therefore $\mathrm{Im}(\phi) \subseteq \mathrm{Ker}(\gamma)$ if and only if $n - 2f + r - k \geq r - s$, i.e. if and only if $k \leq n-2f+s$. So taking $k = n-2f$ we see that $[N, P] \subseteq \mho_k(N)$ and then the desired result follows by using induction on u and the fact that for any $l \geq 0$, $\big[\mho_l(N), P\big] \subseteq \mho_l\big([N, P]\big)$.

□

Proof of Theorem 1. Using the same notation as above we may assume that $|P : N| \geq p^2$ since otherwise P contains a cyclic maximal subgroup and this is the well-known case mentioned in the introduction. Hence if we set $k = \mathrm{cl}(P/N)$ then $1 \leq k \leq 2f - r - 1$ by part i. of Lemma 1, and so using part ii. of Lemma 1 we obtain $P_{k+u+1} \subseteq \mho_{(n-2f)u}(N)$ for any integer $u \geq 1$. So since $|N| = p^{n-2f+r}$ it follows that if u is an integer greater than or equal to 1 and $(n-2f)u \geq n - 2f + r$ then $P_{k+u+1} = 1$. Hence,

$$\begin{aligned} \mathrm{cl}(P) &\leq \mathrm{cl}\left({}^{P}/_{N}\right) + \left\lceil \frac{n-2f+r}{n-2f} \right\rceil + 1 - 1 \\ &= \mathrm{cl}\left({}^{P}/_{N}\right) + \left\lceil \frac{r}{n-2f} \right\rceil + 1, \end{aligned}$$

where the symbol $\lceil x \rceil$ denotes the least integer greater than or equal to x $(\in \mathbb{R})$. Therefore, substituting for $\mathrm{cl}(P/N)$ we have

$$\mathrm{cl}(P) \leq 2f - r - 1 + \left\lceil \frac{r}{n-2f} \right\rceil + 1 = 2f + \left\lceil r\left(\frac{1}{n-2f} - 1\right)\right\rceil \quad (1)$$

which, since $n - 2f \geq 1$ by assumption, is less than or equal to $2f$ as required. □

To prove Theorem 2 we determine the situations under which the right-hand side of (1) actually attains the value $2f$, and show that unless $f(P) = 1$ or $p = 3$ the bound on the class can be improved to $2f(P)-1$. As mentioned in the introduction, there exist groups with $f(P) = 1$ and nilpotency class 2, therefore we will assume $f(P) > 1$ so that (1) applies to any group we consider. We also continue to use the notation already developed above. Observe that there are two possible situations under which the right-hand side of (1) can have the value $2f(P)$:

1. $n - 2f = 1$, i.e. $|P| = p^{2f+1}$.
2. $n - 2f > 1$ and $r = 1$.

Lemma 2 shows that in case 1. the nilpotency class is never equal to $2f$. The proof uses the following standard results on p-groups of maximal class.

Theorem A ([2, III.14.14]) **.** *Let G be a p-group of maximal class and order p^n where $5 \leq n \leq p+1$. Then G/G_{n-1} and G_2 have exponent p.*

Theorem B ([2, III.14.16]) **.** *Let G be a p-group of maximal class and order p^n where $n > p+1$. Then $\mho_1(G_i) = G_{i+p-1}$ for $1 \leq i \leq n-p+1$. Also, G_1 is a regular p-group with $\Omega_1(G_1) = G_{n-p+1}$ and $|G_1/\mho_1(G_1)| = p^{p-1}$.*

Lemma 2. *Let p be an odd prime and P a p-group of coexponent $f = f(P) > 1$ with $|P| = p^n$ where $n = 2f + 1$. Then* $\mathrm{cl}(P) \leq 2f - 1$ *(in particular, P does not have maximal class).*

Proof. Suppose that P does have maximal class $2f$ (for a contradiction) and define Q, N and r as above. Since $r \geq 1$ it follows that $|N| \geq p^2$ and because P has maximal class with $|P : N| \geq p^2$ we know that $N = P_{2f-r}$. Now, $|Q| = p^{f+1} > p^2$ and $n = 2f + 1 \geq 5$, therefore by Theorem A we must have $p < n - 1$, in which case we can apply Theorem B to deduce that P_{n-p+1} has exponent p. Therefore $N \not\subseteq P_{n-p+1}$, i.e. $2 \leq 2f - r < n - p + 1$. We can now apply Theorem A

again with $i = 2f - r$ to obtain

$$\mho_1(N) = P_{2f-r+p-1} \subsetneqq P_{2f-r+1} \tag{2}$$

Since P has maximal class each term of the lower central series has index p in the one above (apart from P_2) and so we must have $|N : P_{2f-r+1}| = p$. But since N is cyclic it has a unique subgroup of index p and so $\mho_1(N) = P_{2f-r+1}$ which contradicts equation (2). $\square$

So we may assume that $n - 2f > 1$ and focus on case 2. above. In this situation the group P/N has order $2f(P)-1$ and contains a cyclic subgroup Q/N which has index $p^{f(P)}$ and trivial core. The next lemma shows that if P/N has maximal class and $f(P) \geq 3$ then we must have $p = 3$. Thus, if we are in case 2. above with $f(P) \geq 3$ and $p > 3$ then 1 can be subtracted from the right-hand side of (1) when substituting for $\mathrm{cl}(P/N)$ thereby bounding the class of P by $2f(P) - 1$. The proof of this lemma uses additional results on p-groups of maximal class, and we indicate where they can be found in Huppert's book [2] as they are used.

Lemma 3. *Let p be an odd prime and G a p-group with $|G| = p^{2k-1}$ where $k \geq 3$. Suppose further that G contains a cyclic subgroup H of index p^k which has trivial core. Then G does not have maximal class except, possibly, when $p = 3$.*

Proof. We consider the two cases $k = 3$ and $k \geq 4$ separately.

a. $k = 3$.
We suppose that $p \geq 5$ and show that $cl(G) \leq 2k - 3 = 3$, so let G be a group of order p^5 which contains a cyclic subgroup H of index p^3 with $\mathrm{Core}_G(H) = 1$. Suppose (for a contradiction) that G has maximal class 4. Then since the hypotheses of Theorem A are satisfied, we know that G/G_4 has exponent p, and because $Z(G) = G_4$ we know that $H \cap G_4 \subseteq \mathrm{Core}_G(H) = 1$. Therefore HG_4/G_4 has order p^2 and is a cyclic subgroup of G/G_4 which contradicts the fact that G/G_4 has exponent p. Hence $cl(G) \leq 3$ as required.

b. $k \geq 4$.

We suppose that G has maximal class $2k-2$ and show that $p = 3$. Since n $(= 2k-1)$ is odd, G is not an exceptional p-group of maximal class (by [2, III.14.6(b)]), i.e. for any i with $2 \leq i \leq n-2$, we have $G_1 = C_G(G_i/G_{i+2})$ where $G_1 = C_G(G_2/G_4)$ (a proper maximal subgroup of G). Therefore by an application of [2, III.14.13(b)] it follows that all elements of G which have order greater than p^2 must lie in G_1. In particular, H and all its conjugates are contained in G_1. So choosing $x \in G$ with $H \cap H^x = 1$ (recall that H has trivial core) we have that $|H||H^x| = p^{2k-2}$. Therefore since G_1 is a (proper) maximal subgroup we have $G_1 = HH^x$. Now because the exponent of G is greater than p^2 we must have $3 \leq p < n-1$ (by Theorem A), and then Theorem B gives us that G_1 is a regular p-group. From the above factorisation of G_1 we can see that $|G_1 : \mho_1(G_1)| \leq p^2$ and $|\Omega_1(G_1)| \geq p^2$, and so by regularity these two inequalities are equalities. Hence $\Omega_1(G_1) = G_{n-2}$ (since $\Omega_1(G_1)$ is a normal subgroup of G and G has maximal class). But we also know by Theorem B that $\Omega_1(G_1) = G_{n-p+1}$, and so $n-p+1 = n-2$, i.e. $p = 3$ as required.

□

We have now shown that Theorem 2 holds for all coexponents greater than 2. Since Lemma 3 is not true for $k = 2$ we deal with the coexponent 2 case directly in the following lemma. The proof of this lemma uses the fact that for a regular p-group, the terms *uniqueness basis* and *type invariants* make sense in direct analogy with finite Abelian p-groups. This result is due to Phillip Hall and the reader should consult [1] for the relevant details.

Lemma 4. *Let p be a prime greater than 3 and P a p-group of coexponent $f(P) = 2$. Then* $\mathrm{cl}(P) \leq 2f(P) - 1$.

Proof. By Theorem 1 the bound $2f(P)$ holds and so since we are assuming $p > 2f(P)$ it follows that $\mathrm{cl}(P) < p$, which implies that P is regular.

Therefore, if we let $|P| = p^n$, P is of *type* $(n-2,2)$ or *type* $(n-2,1,1)$. If P is of *type* $(n-2,2)$ then $|P : \mho_1(P)| = p^2$ and so $[P,P] \subseteq \mho_1(P)$. Therefore $P_3 \subseteq [P, \mho_1(P)] \subseteq \mho_1(P_2) \subseteq \mho_2(P)$. By taking a uniqueness basis of P it is straightforward to see that $\mho_2(P) \subseteq Z(P)$ and therefore $\mathrm{cl}(P) \leq 3 = 2f(P) - 1$. If P is of *type* $(n-2,1,1)$ then the p^{th}-power of a basis element corresponding to the invariant $n-2$ is central, and so $|P : Z(P)| \leq p^3$, from which the required bound follows. □

We have now completed the proof of Theorem 2.

References

[1] P. Hall. A contribution to the theory of groups of prime-power order. *Proc. London Math. Soc.*, **36** (1934) 29–95.

[2] B. Huppert *Endliche Gruppen I*, volume 134 of *Grundlehren Math. Wiss.*, Springer-Verlag, Berline and new York, 1967.

[3] M. lazard. Sur les groupes nilpotents et les anneau de Lie. *Ann. Sci. École Norm. Sup.*, **71** (1954) 101–190.

[4] W. Magnus. Über Gruppen und zugeordnete Liesche Ringe. *J. Reine Angew. Math.*, **182** 1940 142–149.

[5] P.J. Sanders. *Prime-Power Lie Algebras and Finite p-groups*. Ph.D. thesis, University of Warwick, 1994.

Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK

E-mail address: pjs@maths.warwick.ac.uk

Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK